IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

LENORE CALIENDO, individually and on behalf of all others similarly situated, Plaintiff, v. NATIONSBENEFITS, LLC and AETNA INC. Defendants.	Case No. 0:23cv60927 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Lenore Caliendo ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendants NationsBenefits, LLC ("NationsBenefits") and Aetna Inc. ("Aetna" and, together with NationsBenefits, "Defendants"), and complains and alleges upon personal knowledge as to herself and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard her and approximately 3,037,303 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including names, dates of birth, addresses, phone numbers, genders, health plan subscriber identification numbers, Social Security numbers ("SSNs"), and Medicare numbers.

2. NationsBenefits is a company that provides healthcare solutions and supplemental benefits to managed care organizations. The company is headquartered in Plantation, Florida.

3. Aetna is a healthcare benefits company that offers various insurance plans and services to approximately 39 million people. It is headquartered in Hartford, Connecticut.

4. Aetna provides the PII/PHI of its customers to NationsBenefits in connection with insurance or healthcare services. On February 7, 2023, NationsBenefits was notified that Fortra, LLC ("Fortra"), the provider of a file transfer software used by NationsBenefits, experienced a data breach on or about January 30, 2023. Unauthorized individual(s) breached Fortra's network systems and accessed and acquired files containing the PII/PHI of NationsBenefits' and Aetna's customers, including Plaintiff and Class members ("Data Breach").

5. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their customers' PII/PHI from unauthorized access and disclosure.

6. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach.

7. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, breach of fiduciary duty, breach of implied contract, violations of the Illinois Consumer Fraud and Deceptive Practices Act ("ICFA"), and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Lenore Caliendo

8. Plaintiff Lenore Caliendo is a citizen of Illinois.

9. Aetna provides health insurance or related services to Plaintiff. Aetna provided Plaintiff's PII/PHI to NationsBenefits in connection with Plaintiff's health insurance or related services.

10. As a condition of receiving health insurance or related services, Defendants required Plaintiff to provide them with her PII/PHI.

11. Based on representations made by Defendants, Plaintiff believed Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff provided her PII/PHI to Defendants in connection with receiving health insurance or related services.

12. Defendants store and maintain Plaintiff's PII/PHI on their network systems and transmit or share that PII/PII with third parties, including Fortra.

13. Plaintiff takes great care to protect her PII/PHI, including her Medicare information. Had Plaintiff known that Defendants do not adequately protect the PII/PHI in their possession, she would not have obtained services from Defendants or agreed to provide them with her PII/PHI.

14. Plaintiff received a letter from NationsBenefits notifying her that her PII/PHI was exposed in the Data Breach.

15. As a direct result of the Data Breach, Plaintiff has been the victim of medical identity theft. Between January 31, 2023, immediately after the Data Breach, and approximately April 17, 2023, Plaintiff received several bills for medical procedures or tests she did not order or

receive. To date, Plaintiff has been billed over $3,750 for these procedures or tests she neither ordered nor received.

16. As a direct result of the Data Breach, Plaintiff has suffered further injury and damages including, *inter alia*, a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Defendant NationsBenefits, LLC

17. Defendant NationsBenefits, LLC is a Florida corporation with its principal place of business in Plantation, Florida. NationsBenefits headquarters are located at 1801 NW 66th Avenue, Suite 100, Plantation, Florida 33313. It may be served through its registered agent: Caldera Law PLLC, 7293 NW 2nd Avenue, Miami, Florida 33150.

Defendant Aetna Inc.

18. Defendant Aetna Inc. is a Pennsylvania corporation with its headquarters in Hartford, Connecticut. Aetna's headquarters are located at 151 Farmington Avenue, Hartford, Connecticut 06156. Aetna may be served through its registered agent: CT Corporation System, 67 Burnside Avenue, East Hartford, Connecticut 06108.

JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. §1332(d)(2), because: (a) there are 100 or more Class members; (b) at least one Class member is a citizen of a state that is diverse from Defendants; and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

20. This Court has personal jurisdiction over NationsBenefits because NationsBenefits is a Florida corporation and maintains its principal place of business in Florida.

21. This Court has personal jurisdiction over Aetna because Aetna is engaged in substantial business activity in this state, including contracting to insure persons within this state.

22. Venue is proper in this District pursuant to 28 U.S.C. §1391(b)(2) because NationsBenefits' principal place of business is in this District and a significant amount of the events leading to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of NationsBenefits

23. NationsBenefits is "a leading provider of supplemental benefits, flex cards, and member engagement solutions that partners with managed care organizations to provide innovative healthcare solutions."[1] It "offers customizable healthcare solutions through a diverse offering of supplemental benefits that are designed to drive growth, improve outcomes, reduce costs, and delight members."[2]

24. NationsBenefits' website includes a page detailing the Health Insurance Portability and Accountability Act ("HIPAA") rights of its customers.[3] NationsBenefits claims it will share its customers health information to "Treat you," "Run our organization," and "Bill for your services."[4]

[1] *About Us*, NATIONSBENEFITS, https://www.nationsbenefits.com/about-us (last accessed May 16, 2023).
[2] *Outcomes-Based Approach*, NATIONSBENEFITS, https://nationsbenefits.com/outcomes (last accessed May 16, 2023).
[3] *See Your HIPAA Rights*, NATIONSBENEFITS, https://www.nationsbenefits.com/hipaa (last accessed May 16, 2023).
[4] *Id.*

25. NationsBenefits acknowledges it is "required by law to maintain the privacy and security of your protected health information."[5] NationsBenefits promises it "will not use or share your information other than as described here unless you tell us we can in writing."[6]

26. Plaintiff and Class members are, or were, customers of NationsBenefits or health insurance or related services providers, including Aetna who entrusted NationsBenefits with their PII/PHI.

Overview of Aetna

27. "Aetna is the brand name used for products and services provided by one or more of the Aetna group of companies, including Aetna Life Insurance Company and its affiliates."[7] Approximately 39 million people rely on Aetna for health insurance or related services, including medical, pharmacy, and dental plans, and Medicare and Medicaid-related services.[8]

28. Aetna claims to "value the trust you place in us."[9] Aetna states that its customers have a right to "[h]ave your medical records kept private, except when permitted by law or with your approval."[10] Aetna also claims "[p]rotecting the privacy and security of sensitive information is one of our highest priorities."[11]

---

[5] *Id.*
[6] *Id.*
[7] *About Us*, AETNA https://www.aetna.com/about-us.html#:~:text=Aetna%C2%AE%20is%20proud%20to%20be%20part%20of%20the%20CVS%20Health%20family. (last accessed May 16, 2023).
[8] *See Aetna Facts,* Aetna https://www.aetna.com/about-us/aetna-facts-and-companies/aetna-facts.html (last accessed May 16, 2023).
[9] *Aetna's Privacy Center*, AETNA https://www.aetna.com/legal-notices/privacy.html (last accessed May 16, 2023).
[10] *HMO or PPO Rights and Responsibilities*, AETNA https://www.aetna.com/individuals-families/member-rights-resources/rights/hmo-ppo-member-rights.html (last accessed May 16, 2023).
[11] *Aetna's Privacy Center*, *supra* note 9.

29. In its Notice of Privacy Practices, Aetna describes the ways it can use its customers PHI, including for healthcare operations, payment, and treatments.[12] Aetna goes on to claim it will not use its customer's PHI in ways not described within the Notice of Privacy Practices without written permission.[13] Aetna states it "must also follow the terms of the Notice [of Privacy Practices] in effect."[14]

30. Aetna states that its customers have certain rights surrounding their PHI under federal law, and that "[f]ederal privacy law requires us to keep your PHI private."[15] Aetna acknowledges it "must also follow state privacy laws that are stricter (or more protective of your PHI) than federal law."[16]

31. Aetna asserts it uses "administrative, technical and physical safeguards to keep your information from unauthorized access, and other threats and hazards to its security and integrity."[17] Aetna even promises to "continue to protect your information against inappropriate use or disclosure" after a customer's coverage ends.[18] Aetna further claims to "aim beyond the industry standard" when securing PHI.[19]

---

[12] *Notice of Privacy Practices*, AETNA (Feb. 10, 2022), https://www.aetnamedicare.com/content/dam/aetna/pdfs/wwwaetnamedicarecomSSL/individual/2022/member/Notice_of_Privacy_Policies.pdf (last accessed May 16, 2023). Aetna has numerous privacy policies for various plans containing identical or substantially similar statements as those described herein. *E.g.*, https://www.aetna.com/document-library/legal-notices/documents/health-notice-of-privacy-practices.pdf.

[13] *See id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] 17 Steps for Securing Health Information, Aetna https://www.aetna.com/document-library/about-aetna-insurance/document-library/17-steps-securing-health-information.pdf (last accessed May 16, 2023).

The Data Breach

32. NationsBenefits uses software provided by Fortra to exchange files with health plans, including those provided by Aetna.[20] NationsBenefits uploads, stores, transfers, or accesses its customers' PII/PHI using the software provided by Fortra.

33. On or about January 30, 2023, "malicious actor(s) accessed or acquired" files containing the PII/PHI of NationsBenefits customers, including information Aetna provided to NationsBenefits.[21] Fortra notified NationsBenefits of the Data Breach on February 7, 2023.[22]

34. NationsBenefits began notifying affected persons of the Data Breach on or about April 13, 2023, over two months after learning of the Data Breach.[23] The notice letter NationsBenefits sent to Class members states the information affected by the breach includes Class members' "First Name; Last Name; Gender; Health Plan Subscriber Identification Number; Social Security Number; Address; Phone Number; Date of Birth; [and] Medicare Number."[24]

Defendants Knew that Criminals Target PII/PHI

35. At all relevant times, Defendants knew, or should have known, that the PII/PHI that they collected, shared, and stored was a target for malicious actors. Aetna warns its customers that "[t]hieves often steal Social Security numbers when they hack websites and computers."[25] Aetna

---

[20] *See Notice Letter*, Aetna (Apr. 28, 2023), available at https://apps.web.maine.gov/online/aeviewer/ME/40/cc06cdee-0715-4eea-8b33-c391dba8fe5e.shtml (under "Notification and Protection Services" click link titled "Live Proof_L07_Redacted").
[21] *See id.*
[22] *Id.*
[23] *See* NationsBenefits Data Breach Notification, ME. ATT'Y GEN. (May 5, 2023), https://apps.web.maine.gov/online/aeviewer/ME/40/cc06cdee-0715-4eea-8b33-c391dba8fe5e.shtml. April 13, 2023 was the earliest date NationsBenefits sent notice to some Class members; it did not send notice to some Class members until April 27 and 28, 2023. *See id.*
[24] *Notice Letter*, *supra* note 19.
[25] *Aetna's Privacy Center*, *supra* note 9.

similarly warns of the risk of medical identity theft and acknowledges "it's happening more and more in the United States."[26] NationsBenefits is clearly aware of the threat of a data breach, as it promises to "let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[27]

36. Defendants knew or should have known of these risks. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Defendants should have anticipated and guarded against.

37. It is well known amongst companies that store sensitive PII that sensitive information – such as the SSNs and medical information stolen in the Data Breach – is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[28]

38. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[29] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[30]

---

[26] *Id.*
[27] *Your HIPAA Rights*, *supra* note 3.
[28] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[29] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Apr. 26, 2023).
[30] *See id*.

39. PII/PHI is a valuable property right.[31] The value of PII/PHI as a commodity is measurable.[32] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[33] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[34] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

40. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

---

[31] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[32] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[33] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[34] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

41. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[35] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[36]

42. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[37] According to a report released by the Federal Bureau of Investigation's Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen SSN or credit card number.[38]

43. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[39] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information – specifically, regarding a sexually transmitted disease or terminal illness – that information can be used to extort or coerce someone to do what you want them to do."[40]

---

[35] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[36] *Id.*

[37] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[38] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[39] *What Happens to Stolen Healthcare Data*, *supra* note 27.

[40] *Id.*

44. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[41]

45. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has, thus, deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

46. Theft of PII/PHI is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[42]

47. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[43] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is

[41] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[42] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Apr. 26, 2023).

[43] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[44]

48. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[45]

49. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[46]

50. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[44] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Apr. 26, 2022).

[45] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Apr. 26, 2023).

[46] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Apr. 26, 2022).

51. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII *(e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. *TIME Magazine* quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[47]

52. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[48] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[49] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [50] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[51]

53. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

---

[47] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[48] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[49] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* note 30.
[50] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Apr. 26, 2023).
[51] *Id*.

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

- Significant bills for medical goods and services neither sought nor received.

- Issues with insurance, co-pays, and insurance caps.

- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[52]

54. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[53]

55. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of

[52] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* note 40.
[53] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

56. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (a) a substantially increased and imminent risk of identity theft; (b) the compromise, publication, and theft of their PII/PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (d) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (e) the continued risk to their PII/PHI which remains in Defendants' possession; (f) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (g) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

57. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

58. Plaintiff brings this action on behalf of herself and all members of the following Nationwide Class of similarly situated persons:

> All persons whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

59. The Nationwide Class asserts claims against Defendants for negligence, breach of fiduciary duty, breach of implied contract, and unjust enrichment.

60. Alternatively, pursuant to Fed. R. Civ. P. 23(c)(5), Plaintiff brings this action on behalf of herself and a subclass consisting of all members of the following Illinois Class of similarly situated persons:

> All Illinois residents whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all Illinois residents who were sent a notice of the Data Breach.

61. The Illinois Class asserts a claim under the Illinois Consumer Fraud and Deceptive Practices Act ("ICFA"), 815 ILCS 505/1, *et seq.*

62. Excluded from the Classes are NationsBenefits, LLC, and its affiliates, parents, subsidiaries, officers, agents, and directors; Aetna Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors; as well as the judge(s) presiding over this matter and the clerks of said judge(s).

63. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

64. The members of the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. NationsBenefits reported to the United States Department of Health and Human Services that approximately 3,037,303 persons' information was exposed in the Data Breach.[54]

65. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

[54] *See Breach Portal*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed May 16, 2023).

a. whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

f. whether Defendants breached their duties to protect Plaintiff's and Class members' PII/PHI; and

g. whether Plaintiff and Class members are entitled to damages, and the measure of such damages and relief.

66. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

67. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

68. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that

conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

69. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

70. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

71. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding, securing, and protecting the PII/PHI in their possession, custody, or control.

72. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining and using

secure systems. Defendants knew or should have known of the many data breaches that have targeted companies that stored PII/PHI in recent years.

73. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified and foreseen that the third parties they share information with could have vulnerabilities in their systems and prevented the dissemination of Plaintiff's and Class members' PII/PHI.

74. Defendants make explicit statements on their websites that they are aware of the risk of potential data breaches, that they will follow privacy laws and regulations, and that they will use reasonable methods to protect the PII/PHI in their control.

75. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to ensure that the third parties they share PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiff's and Class members' PII/PHI.

76. Plaintiff and Class members had no ability to protect their PII/PHI that was, or remains, in NationsBenefits' or Aetna's possession.

77. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to ensure that the third parties they share PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the

unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

78. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised. The PII/PHI of Plaintiff and the Class was accessed and stolen as the proximate result of Defendants' failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, ensuring that third parties they contract with and share PII/PHI with adopt, implement, and maintain appropriate security measures.

79. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (a) a substantially increased and imminent risk of identity theft; (b) the compromise, publication, and theft of their PII/PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (d) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (e) the continued risk to their PII/PHI which remains in Defendants' possession; (f) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (g) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF FIDUCIARY DUTY

80. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

81. As a condition of obtaining services or employment from Defendants, Plaintiff and Class members gave Defendants their PII/PHI in confidence, believing that Defendants would protect that information. Plaintiff and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Defendants and Plaintiff and Class members. In light of this relationship, Defendants must act primarily for the benefit of their customers, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

82. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. They breached that duty by failing to ensure that the third parties they contract with and share PII/PHI with properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that they collected, shared, and stored.

83. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (a) a substantially increased and imminent risk of identity theft; (b) the compromise, publication, and theft of their PII/PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (d) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (e) the continued risk to their PII/PHI which remains in NationsBenefits' and Aetna's possession; (f) future costs in terms of time, effort, and money that will be required to prevent,

detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (g) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT

84. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

85. In connection with receiving health care services or employment, Plaintiff and all other Class members entered into implied contracts with Defendants.

86. Pursuant to these implied contracts, Plaintiff and Class members benefited Defendants by paying monies to Defendants, and provided Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and Plaintiff understood that Defendants would: (a) provide health insurance or related benefits, products, or services, to Plaintiff and Class members; (b) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; (c) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards; and (d) ensure third parties they contract with and share PII/PHI with implement and maintain reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI.

87. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendants, on the other hand. Indeed, as set forth *supra*, Defendants recognized the importance of data security and the privacy of their customers' PII/PHI. Had Plaintiff and Class members known that Defendants would not adequately protect their PII/PHI, they would not have paid for products or services from Defendants.

88. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendants with their PII/PHI and paid monies for products and services from Defendants, expecting that their PII/PHI would be protected.

89. Defendants breached their obligations under their implied contracts with Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to ensure that the third parties they contract with and share PII/PHI with implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

90. Defendants' breach of their obligations of the implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiff and Class members.

91. Plaintiff and all other Class members were damaged by Defendants' breach of implied contracts because: (a) they paid monies (directly or indirectly) to Defendants in exchange for data security protection they did not receive; (b) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (c) their PII/PHI was improperly disclosed to unauthorized individuals; (d) the confidentiality of their PII/PHI has been breached; (e) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (f) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (g) they overpaid for the services that were received without adequate data security.

COUNT IV
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE PRACTICES ACT, 815 ILL. COMP. STAT. 505/1, *et seq.*
(on behalf of the alternative Illinois Class)

92. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

93. NationsBenefits and Aetna as corporations, are "persons" as defined in the ICFA, 815 ILL. COMP. STAT. 505/1(c), and Illinois Uniform Deceptive Trade Practices Act ("IUDTPA:), 815 ILL. COMP. STAT. 510/1(5).

94. The services, benefits, and products provided or sold by NationsBenefits and Aetna are "merchandise" as defined in the ICFA. *See* 815 ILL. COMP. STAT. 505/1(b).

95. Defendants' sale of health insurance or related benefits and services to Plaintiff and Class members is "trade" or "commerce" under the ICFA. *See* 815 ILL. COMP. STAT. 505/1(f).

96. The ICFA declares any "[u]nfair methods of competition and unfair or deceptive acts or practices, including but not limited to . . . any deception[,] fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact" to be unlawful. 815 ILL. COMP. STAT. 505/2. The ICFA also declares the use or employment of any practice described in the "IUDTPA", 815 ILL. COMP. STAT. 510/2, to be unlawful. *Id.*

97. Under the IUDTPA, a person engages in a deceptive trade practice when, *inter alia*, the person "represents that goods or services have . . . characteristics. . . uses, [or] benefits . . . that they do not have," 815 ILL. COMP. STAT. 510/2(5); "represents that . . . services are of a particular standard, quality, or grade . . . if they are of another," 815 ILL. COMP. STAT.

510/2(7); or "advertises goods or services with intent not to sell them as advertised," 815 ILL. COMP. STAT. 510/2(9).

98. Plaintiff and Illinois Class members purchased and received health insurance or related benefits, products, or services from Defendants for personal, family, or household purposes.

99. Defendants made explicit statements and other representations to their customers that they would ensure the security and integrity of their customers' PII/PHI, and that their customers' PII/PHI would remain private. Defendants made these representations in the conduct of trade or commerce and with the intent that Plaintiff and Illinois Class members rely on those representations.

100. The goods or services sold by Defendants did not have the characteristics, benefits, or qualities that Defendants represented them to have, in violation of the ICFA.

101. Defendants also engaged in unlawful and unfair practices in violation of the ICFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiff and Class members' PII/PHI, and in failing to ensure that the third parties they contract with and share PII/PHI with implement and maintain security protocols and procedures to protect Plaintiff's and Illinois Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

102. Defendants further violated the ICFA by failing to notify their customers of the Data Breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILL. COMP. STAT. 530/10. Violation of the

Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILL. COMP. STAT. 530/20.

103. Due to the Data Breach, Plaintiff and Illinois Class members have lost property in the form of their PII/PHI. Further, Defendants' failures to implement and maintain reasonable security measures to protect and secure Plaintiff and Illinois Class members' PII/PHI, and failure to ensure that the third parties they contract with and share PII/PHI with implement and maintain security protocols and procedures to protect Plaintiff's and Illinois Class members' PII/PHI, will force Plaintiff and Illinois Class members to spend time or money to protect against identity theft. Plaintiff and Illinois Class members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting, sharing, and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

104. As a result of Defendants' violations of the ICFA, Plaintiff and Illinois Class members have suffered and will suffer injury, including, but not limited to: (a) a substantially increase or imminent risk of identity theft or medical identity; (b) the compromise, publication, and theft of their PII/PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (d) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (e) the continued risk to their PII/PHI which remains in Defendants' possession; (f) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (g) overpayment for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

105. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

106. This claim is pleaded in the alternative to the breach of implied contract claim.

107. In obtaining services from Defendants, Plaintiff and Class members provided and entrusted their PII and PHI to Defendants.

108. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid for health insurance or related benefits or services with an implicit understanding that Defendants would use some of their revenue to protect the PII/PHI they collect, share, and store.

109. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing and payment services, which enabled Defendants to carry out their business.

110. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for and expected, and those payments without reasonable data privacy and security practices and procedures that they received.

111. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves and the third parties that they contract with and share PII/PHI with that

Plaintiff and Class members paid for and expected, and that were otherwise mandated by federal, state, and local laws and industry standards.

112. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds they received as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

DATED: May 18, 2023

ROBBINS GELLER RUDMAN
& DOWD LLP
STUART A. DAVIDSON (FBN 84824)
DOROTHY P. ANTULLIS (FBN 890421)
ALEX C. COHEN (FBN 1002715)
BRADLEY M. BEALL (FBN 1010635)
ANNY M. MARTIN (FBN 1000491)

s/ STUART A DAVIDSON
STUART A. DAVIDSON

225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364(fax)
sdavidson@rgrdlaw.com
dantullis@rgrdlaw.com
acohen@rgrdlaw.com
bbeall@rgrdlaw.com
amartin@rgrdlaw.com

BARNOW AND ASSOCIATES, P.C.
Ben Barnow*
Anthony L. Parkhill*
205 West Randolph Street, Suite. 1630
Chicago, IL 60606
Telephone: 312/621-2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

**Pro hac vice forthcoming*

Attorneys for Plaintiff